(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－325372
（P2001－325372A）
(43)公開日　平成13年11月22日(2001.11.22)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　17/60	１２６	Ｇ０６Ｆ　17/60	１２６Ｚ	
Ａ６１Ｂ　5/00		Ａ６１Ｂ　5/00	Ｇ	

審査請求　未請求　請求項の数４　ＯＬ　（全９頁）

(21)出願番号　特願2001－64444(P2001－64444)

(22)出願日　平成13年３月８日(2001.3.8)

(31)優先権主張番号　特願2000－63044(P2000－63044)
(32)優先日　平成12年３月８日(2000.3.8)
(33)優先権主張国　日本（ＪＰ）

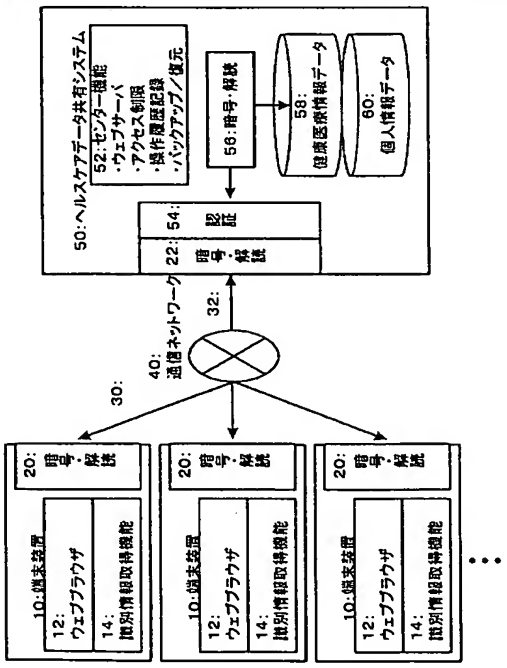
(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(72)発明者　杉村　幸彦
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　中尾　成隆
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(74)代理人　100109852
弁理士　岩田　茂

最終頁に続く

(54)【発明の名称】　ヘルスケアデータ共有システム，ヘルスケアデータ共有方法およびヘルスケアデータ共有プログラム

(57)【要約】
【課題】　個人の健康医療情報は、個人が診療を受けた医療機関、健康診断を受けた学校／企業／健診センターなどがそれぞれに保管しており、本来健康医療情報の所有者である本人であっても情報の入手が困難であった。
【解決手段】　個人が診療を受けた医療機関、健康診断を受けた学校／企業／健診センターなどがそれぞれに保管していた個人の健康医療情報を、ネットワーク上のヘルスケアデータ共有システムに集約して管理する。

通信ネットワークを介してアクセス可能なヘルスケアデータ共有システムの説明図



1

【特許請求の範囲】

【請求項１】　個人の健康医療情報を電子データとして管理するデータ管理機能、利用者の権限および要求に応じ個人の健康医療情報データの一部ないし全てをネットワーク経由でアクセスできるアクセス機能を有し、健康医療情報データを共有できることを特徴とするヘルスケアデータ共有システム。

【請求項２】前記個人の健康医療情報の電子データを管理するデータ管理センターを設け、健康医療情報データを集中管理し、

前記ヘルスケアデータ共有システムから取得した前記個人の健康医療情報データを、追加、削除、更新を行うデータ追加機能、データ削除機能、データ更新機能の少なくとも１つを設け、個人健康情報データの追加、削除、更新の少なくとも１つができ、

前記データ追加機能、データ削除機能、データ更新機能の少なくとも１つを端末装置側に設け、

前記個人の健康医療情報データにアクセスしデータの取得、追加、削除、更新を行った場合、操作を行った利用者および日時などを特定できる操作記録機能を設け、データのアクセス内容、操作した利用者、操作日時の少なくとも１つの履歴が判るようにし、

前記操作した利用者の情報にヘルスケアデータ共有システム利用者認証を使用する操作者認識機能を設け、操作した利用者の特定をし、

前記利用者の権限を管理する利用者権限機能を設け、その権限に応じヘルスケアデータ共有システムから取得できる情報、操作内容を制限し、

前記個人の健康医療情報データに、診療データ、服薬データ、健康診断データおよび生体情報データの一部または全てを管理する各データ管理機能を設け、利用者の権限、要求によりデータの取得、追加、削除、更新でき、

前記個人の健康医療情報データの他に個人に関わる情報（例えば家族歴、遺伝子情報等）の一部または全てを管理する個人情報管理機能を設け、利用者の権限、要求によりデータの取得、追加、削除、更新ができ、

前記個人の健康医療情報データの一部または全てを暗号化しデータを管理するデータ暗号化管理機能と、データをデータ管理機能より取得する際に暗号を解読するデータ解読管理機能を設け、前記データ管理センターでのデータのセキュリティを高め、

前記個人の健康医療情報データを通信ネットワーク経由で送受信する際に、送信するデータの一部または全てを暗号化するデータ暗号化機能と、受信した暗号データを解読するデータ解読機能を、端末装置とヘルスケアデータ共有システムの両方に設け、前記通信ネットワーク上でのデータのセキュリティを高め、

前記利用者が自分の健康医療情報データのセキュリティレベルを選択出来るセキュリティ選択機能を設け、健康医療情報データの一部ないし全ての暗号化有無を各自で

2

設定でき、

前記利用者の健康保険番号、クレジットカード等の情報を管理する健康保険管理、カード情報管理機能を設け、医療会計事務処理を行うことができ、

前記個人の健康医療情報データの抽出、分析機能を設け、データの分析を行うことができることを特徴とする請求項１記載のヘルスケアデータ共有システム。

【請求項３】　個人の健康医療情報を電子データとして保存する健康医療情報データベースと、該健康医療情報データベースのアクセス制限を管理し、該健康医療情報データベースへの少なくとも記録を含む操作履歴を記録する操作履歴記録可能なセンター機能と、該健康医療情報データベースを利用する利用者を特定する認証機能と、通信ネットワーク経由で送受信するデータを暗号化および復号化するデータ暗号化機能とを有するヘルスケアデータ共有システムにおいて、

前記通信ネットワークを経由してアクセスしてくる利用者を認証し、

認証した利用者に対するアクセス制限の範囲で前記健康医療情報データベースの情報を暗号化して送信し、

該送信した情報に対して追加、削除、更新された編集情報を受信して復号化して前記健康医療情報データベースに保存すると共に、前記認証機能で特定した利用者の操作履歴として記録することを特徴とするヘルスケアデータ共有方法。

【請求項４】　個人の健康医療情報を電子データとして保存するヘルスケアデータ共有システムにアクセスするログインステップと、

前記健康医療情報にアクセスする利用者を設定する利用者設定ステップと、

前記ヘルスケアデータ共有システムから暗号化して送信されてきた健康医療情報データを復号化して表示する表示ステップと、

前記表示された健康医療情報データを編集して、該編集した結果を暗号化して前記ヘルスケアデータ共有システムへ送信する送信ステップとからなることを特徴とするヘルスケアデータ共有プログラム

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、医療分野において、個人の健康医療情報を電子データとして管理し、利用者の権限および要求に応じ、個人の健康医療情報データの一部ないし全てを、ネットワーク経由でアクセスできる機能を有するヘルスケアデータ共有システムに関するものである。

【０００２】

【従来の技術】近年規制緩和により、例えば診療録の記録および保存が紙のみならず、電子媒体でも可能となった。これにより、紙のバックアップ程度しか機能していなかった電子的な診療録が、紙に変わる記録および保存

手段として導入されつつある。

【０００３】

【発明が解決しようとする課題】従来、個人の健康医療情報は、個人が診療を受けた医療機関、健康診断を受けた学校／企業／健診センターなどがそれぞれに保管しており、本来健康医療情報の所有者である本人であっても情報の入手が困難であった。

【０００４】さらに健康医療情報は、保管機関により情報が記載された媒体、フォーマットが異なり、情報の共有が困難であった。さらに、提携した病院同士ではネットワークを介して情報の提供を行なえる場合もあるが、極限られた範囲での情報の共有であり一般的でない上に、健康医療情報の所有者である本人が情報を入手できるものではなく、医師同士など、医療機関のスタッフ同士での情報の共有しか行えない。また、健康医療情報の所有者が主体的に情報の使用権限を設定することができなかった。

【０００５】

【課題を解決するための手段】従来、個人が診療を受けた医療機関、健康診断を受けた学校／企業／健診センターなどがそれぞれに保管していた個人の健康医療情報を、ネットワーク上のヘルスケアデータ共有システムに集約して管理する。また、情報が記載された媒体、フォーマットを統一することで、ネットワークを介して情報を共有できるだけでなく、異なるシステム間においても健康医療情報データの共有を行うことが可能となる。さらに、健康医療情報の所有者が主体的に情報の使用権限を設定することにより、本人による健康医療情報の管理が可能になる。

【０００６】それぞれに識別情報を有する利用者が使用する端末装置と、該端末装置とネットワークで接続されたヘルスケアデータ共有システムであって、前記のヘルスケアデータ共有システムは、健康医療情報を管理する手段と、前記情報をネットワーク経由でアクセス出来る手段と、前記情報をネットワーク経由でアクセスした際の、データのアクセス内容、操作者、操作日時の少なくとも１つの履歴が判る手段と、前記端末装置から受信した識別情報と保持している識別情報から利用者の特定を行う手段と、利用者の権限を設定する手段と、利用者の権限に応じたデータの取得、追加、削除、更新のアクセス制限を実現する手段と、ネットワークの伝送路においてデータの暗号化と解読を行う手段と、データの一部または全てを暗号化して保存し、それらを解読する手段と、データの一部または全てをバックアップし、必要に応じて復元する手段と、利用者の所有するデータを検索しデータを抽出する手段と、前記抽出したデータを分析する手段と、を備えていることができる。

【０００７】また前記のヘルスケアデータ共有システムは、個人の健康保険番号、カード情報を保有し、医療会計事務処理を行う手段と、データを所有する利用者本人

が他の利用者に自分のデータの取得、追加、削除、更新の権限を与えることができる手段と、データを所有する利用者本人以外の、特別な権限を持つ他の利用者が、個人情報以外の健康医療情報データを検索し、データを抽出する手段と、を備えることもできる。

【０００８】また、前記端末装置は、利用者が識別情報をヘルスケアデータ共有システムに送信する手段と、利用者が健康医療情報データにアクセスする手段と、ネットワークの伝送路におけるデータの暗号化と解読を行う手段と、を備えている。さらに、前記健康医療情報データには、診療データ、服薬データ、健康診断データ、生体情報データ、などが含まれる。さらに、前記個人に関わる情報には家族歴、遺伝子情報などが含まれる。さらに、前記個人情報には氏名、生年月日、住所、電話番号、識別情報、健康保険番号、支払いクレジットカード番号などが含まれる。さらに、前記権限は患者、医師、看護婦、薬剤師、病院事務、システム管理者、データ管理者、などを設定でき、さらに、前記識別情報には利用者アカウントとパスワード、指紋情報、虹彩情報、音声情報、筆跡情報などの一部または全てを設定することもできる。

【０００９】

【発明の実施の形態】図１に本発明の実施の形態を示す。図１には通信ネットワーク４０を介してアクセス可能なヘルスケアデータ共有システムの一実施例を示す。通信ネットワーク４０はインターネット通信プロトコルによって可能となるワールドワイドウェブ通信を表す。ヘルスケアデータ共有システム５０は、センター機能５２、認証機能５４、暗号解読機能５６、健康医療情報データベース５８、個人情報データベース６０、および、暗号解読機能２２を有する。一方端末装置１０はウェブブラウザ１２、識別情報取得機能１４、暗号解読機能２０を有する。

【００１０】センター機能５２は、ウェブサーバ機能、アクセス制限機能、操作歴記録機能、バックアップ復元機能を有する。ウェブサーバ機能は、より多くの端末装置でヘルスケアデータを共有できるように、ウェブブラウザで参照可能な形態に健康医療情報データをＨＴＭＬ文書としてＨＴＴＰプロトコルで出力する。アクセス制限機能は認証した結果に基づいて参照可能な健康医療情報データの範囲や記録可能な健康医療情報データ範囲を管理する。操作歴記録機能は、健康医療情報データを記録する際に操作した利用者の特定を可能な情報および操作した時刻情報を保存する。バックアップ復元機能は、健康医療情報データベース５８に蓄積された情報を例えばテープやＣＤＲのような可搬媒体に定期的にバックアップを行い、健康医療情報データベース５８が復旧不可能な障害が発生した場合に、前述の可搬媒体から健康医療情報データベース５８を復元する。認証機能５４はアクセスしてきている利用者が登録されている者か、ある

5

いは、現在のアクセスが正常に認証されたアクセスなのか判定する。

【００１１】暗号解読機能５６は健康医療情報データベース５８のデータが万が一にも外部に漏れた際に内容を判読できないようにし、さらに、健康医療情報データベース５８と個人情報データベース６０の双方のデータが万が一にも外部に漏れた際に、これら２つのデータベース間のデータの整合性をとれないように、暗号化してデータベースに保存し、読み出す際には解読して読み出す。健康医療情報データベース５８は、患者が共有したいヘルスケアデータが保存されている。個人情報データベース６０はクレジットカードの番号や保険証の番号など、決算に必要な情報　を含める個人の情報が保存されている。

【００１２】暗号解読機能２０および２２は、通信ネットワーク上でのデータのセキュリティを保証するために、通信ネットワークへデータを送出する際には暗号化を行い、通信ネットワークからデータを受信する際には解読を行なう。ウェブブラウザ１２は、ヘルスケアデータ共有システムから送信されてきた健康医療情報データを表示する。識別情報取得機能１４は端末装置１０を利用している利用者を特定するための情報を認証機能５４とやりとりする。

【００１３】ヘルスケアデータ共有システム５０と端末装置１０はそれぞれ通信経路３０および３２を用いてインターネットにアクセスする。通信経路３０および３２はインターネットへの直接接続でもよく、またインターネットへのアクセスを提供するインターネットサービスプロバイダへの接続であってもよい。また、ヘルスケアデータ共有装置５０は、アウトソーシング事業を行うような事業者あるいは、ホームページサービスを行うような事業者であることが望ましい。これらの事業者は、通常インターネットにアクセスするネットワークの帯域幅が広く、ネットワーク犯罪に対する設備や自然災害に対する設備などに関しても病院で導入できる情報設備に比べて高度な情報保護が可能となる。

【００１４】さらに、病院と患者以外の第三者的な事業者であることから、カルテ情報の隠蔽や改竄をさらに行いにくくなり、データの信頼性がさらに向上する。このことから、例えば医療機関でこのような事業者に対応できることをアピールすれば、情報開示に対する準備が整っていることの証明になり、その医療機関は医療的な処置のみならず、情報に関する信頼をも患者へ提供することができる。さらに、このような事業者には、医療情報という観点について、以下の点を考慮するのみで実現できることから現実的である。

【００１５】（１）保存義務のある情報の真正性が確保されていること。

○故意または過失による虚偽入力、書換え、消去および混同を防止すること。

6

○作成の責任の所在を明確にすること。

【００１６】（２）保存義務のある情報の見読性が確保されていること。

○情報の内容を必要に応じて肉眼で見読可能な状態に容易にできること。

○情報の内容を必要に応じて直ちに書面に表示できること。

【００１７】（３）保存義務のある情報の保存性が確保されていること。

○法令に定める保存期間内、復元可能な状態で保存されていること。

【００１８】特に、（２）および（３）については、上記の事業者が容易にあるいは既に実現できていることであり、上記の事業者は本発明の実施が容易である。また、端末装置１０として携帯電話、PHSなどの携帯情報端末を利用したインターネットへのアクセスでもよい。

【００１９】本実施形態においてインターネットにアクセス可能な医療機関、健診センター、学校、企業、店舗などの任意の場所にいる医師、看護婦、あるいはその他のヘルスケアサービス従事者および患者、健康診断受診者などの利用者は、端末装置１０を用いてヘルスケアデータ共有装置にアクセスすることができる。

【００２０】利用者は、端末装置１０の識別情報送信機能１４によりヘルスケアデータ共有システムに暗号化機能２０で暗号化した識別情報を送信する。ヘルスケアデータ共有システム５０は、利用者認証機能５４により、暗号解読機能２２で解読した識別情報を個人情報データ６０に含まれる識別情報と照合し認証を行う。認証に成功した場合に利用者はヘルスケア共有システム５０にアクセス可能となる。

【００２１】ヘルスケアデータ共有システム５０は、センター機能５２により利用者の権限に応じたデータのアクセス制限を行う。またこのとき健康医療情報データの重要度や利用者の設定に応じて、データ暗号化／解読機能５６により、適宜健康医療情報データの暗号化／解読を行う。さらに、端末装置１０にデータを送信する際にも健康医療情報データ５８の重要度や利用者の設定に応じて、暗号化機能２２により暗号化通信を行うことができ、端末装置１０では受信したデータが暗号化されている場合には、解読機能２０によりデータの解読をおこない、ウェブブラウザ１２で内容を表示する。

【００２２】例えば患者が医療機関で診察を受ける場合には、患者はヘルスケアデータ共有システム５０に接続し認証を行い、認証後に医療機関での利用者である担当医師に自分の健康医療情報データ５８に診察結果データを追加する権限を与える。このとき担当医師はヘルスケアデータ共有システム５０に接続し認証を行った後に、患者の健康医療情報データ５８に診察データを追加することができる。患者は医師の診察結果データを確認し、必要に応じてセンター機能５２でセキュリティ設定を行

7

う。

【００２３】これらの作業を行う際に、ヘルスケアデータ共有システムを運用する事業者や病院などから発行されるICカードや、ICカード状の健康保険証などに、患者が契約しているヘルスケアデータ共有システムの情報(例えばhttps://provider.net/accountといったネットワーク上のアドレス情報や利用者アカウントやパスワードなど)を登録しておけば、何度も同じことを入力する手間が省けて便利である。また上記の例では、利用者個人の権限を個別に個人情報データ６０へ登録する場合を説明したが、多数の利用者の資格を一括して登録されたデータベースなどを選択指定できるようにしてもよく、そのデータベースは例えば医療機関で働くスタッフを登録したようなデータベースを各医療機関で用意しておくこともできるし、医療機関外の事業者に委託して用意することもできる。このようなデータベースを用いれば、医療機関へ行った際に受付,診察,会計といった場面で何度も認証を行う必要がなくなり便利である。

【００２４】個人の健康医療情報をネットワーク上のヘルスケアデータ共有システムに集約して管理することにより、利用者の権限に応じたアクセス制限のもとで情報の共有化が図れる。また統一された電子データフォーマットで保管されているので、情報の入手、使用が容易である。これにより、例えばかかりつけの病院以外で受けた健康診断情報を病院で参照することができたり、検査などの大きな設備を伴うことのみ医療機関へ出向きそれ以外は近所の診療所や薬局で処置を済ませることも容易となる。さらに薬局では、過去の薬歴を参照できることで、アレルギーなどの情報を参照したり、クレジットカードなどの決済情報を入手することができることから、例えば単に風邪薬を購入する場合にも口頭で説明した以上のサービスを受けることができる。さらに、定型的な問診表は、医療機関へ出向く前に自宅で、自分が利用者となって登録しておくことで、医療機関での受付を容易にし、受付待ちによる負担を減少することもできる。

【００２５】さらにデータをデータセンターで保管することにより、災害時のデータ保護、盗難防止等が行え、セキュリティと安全性を高めることができる。また、健康医療情報データを個人情報データと別のデータベースにして管理することで、万一健康医療情報データが漏洩したとしても、誰の健康医療情報であるかを特定することができないため、情報の価値が無くなり、セキュリティと安全性を高めることができる。

【００２６】図２～図４は本発明のヘルスケアデータ共有システムを実施した際の一例を示すもので、表示される画面例を表している。また、図５はヘルスケアデータ共有システムを利用するフローを示す図である。

【００２７】まず図５のステップＳ１０１のログイン処理を説明する。患者は病院や薬局など、ヘルスケアデータ共有システムを利用したい場所に出向き、そこにある

8

パソコンで図４に示すようなウェブブラウザ１２０を起動し、患者の健康医療情報データが格納されたデータセンターのインターネット上のアドレスを入力する。ウェブブラウザはこのアドレスにアクセスし、通信ネットワーク上のデータのセキュリティを確保するための暗号化処理を実施して通信を開始する。

【００２８】通信を開始すると、データセンターからユーザ名とパスワードの入力を要求され、図２に示すような入力画面１００を表示する。入力画面１００には、ユーザ名を入力するユーザ名入力欄１０１と、パスワードを入力するパスワード入力欄１０２と、入力した結果を送信するＯＫアイコン１０３と、ユーザ名とパスワードの入力をキャンセルするキャンセルアイコン１０４が設けられている。

【００２９】ユーザ名入力欄１０１には、データセンターから発行されたアカウントを入力し、パスワード入力欄１０２にはそのアカウントに対するパスワードを入力する。パスワードの入力は入力された文字が「＊」等の記号に置きかわって表示することで入力された文字をマスクする。ユーザ名とパスワードの入力が完了したらＯＫアイコン１０３をクリックする。ＯＫアイコン１０３がクリックされるとウェブブラウザはユーザ名とパスワードを暗号化してデータセンターに送信する。また、キャンセルアイコン１０４をクリックした場合にもユーザ名とパスワード無しとしてデータセンターに送信する。

【００３０】データセンターは送信されてきたユーザ名とパスワードの暗号を解読して認証し、アクセスしようとしているアドレスに許可されたユーザ名とパスワードか認証する。認証に失敗した場合は、アドレスが正しいかどうかの確認を促すメッセージと共にデータセンターの連絡先を記載したページを送信し、認証に成功した場合は利用者の設定に移る。データセンターは利用者設定用のページを暗号化して送信する。

【００３１】次に図５のステップＳ１０２の利用者の設定処理を説明する。利用者設定用のページを受信したウェブブラウザは暗号化されたページを解読して、図３に示すような新たなウィンドウ１１０を表示する。ウィンドウ１１０には、利用者名の入力欄１１１，パスワードの入力欄１１２，利用者権限の選択欄１１３，プルダウンメニュー１１４，ＯＫアイコン１１５が設けられており、利用者名や利用者権限のように、既に登録されている内容を選択可能な場合はプルダウンメニューとして送信されてくる。

【００３２】利用者はこの画面で利用者名の入力欄１１１の右端のプルダウンメニューをクリックしてメニューを表示し、既に登録してある自分の名前を選択し、パスワード入力欄１１２にパスワードを入力してＯＫアイコン１１５をクリックする。

【００３３】あるいは利用者名の入力欄１１１に利用者名を入力することで、利用者の登録が可能となる。利用

者の登録を行なう場合は、登録する利用者名を利用者名の入力欄１１１に入力し、利用者登録用のパスワードをパスワード入力欄１１２に入力し、利用者権限を利用者権限選択欄１１３のプルダウンメニュー１１４から選択してＯＫアイコン１１５をクリックする。次に、新たな利用者の登録に必要なパスワードの入力欄や必要に応じて発行できる利用者アカウントの発行の確認欄がある登録画面が表示される。

【００３４】利用者の設定画面で入力されたデータは暗号化されデータセンターに送信されデータセンターで解読され認証される。データセンターは利用者を認証することで、現在アクセスしてきているアドレスの権限を設定する。これにより、その利用者が参照可能な患者の健康医療情報データのみを暗号化して送信し、さらに、受信して解読した健康医療情報データのうち、その利用者の権限の範囲内のデータのみ、利用者を特定可能な情報と共に保存する。

【００３５】図５のステップＳ１０３のヘルスケアデータの表示処理を説明する。図４は利用者に応じてデータセンターから送信されて来たページを解読して表示した内容を示しており、ウェブブラウザ１２０に、患者の健康医療情報データ１２１と、患者の健康医療情報データの編集欄１２２が表示されている。

【００３６】利用者が薬剤師の場合は、患者の健康医療情報データ１２１を参照して過去の処方歴やアレルギーなどを参照して調剤し、患者に最も適した薬を提供することが可能となる。

【００３７】利用者が医師の場合には、患者の健康医療情報データ１２１を参照して他の病院での診療歴などを参照診断することが可能となる。

【００３８】図５のステップＳ１０４の入力されたヘルスケアデータの送信処理を説明する。医師が診療した結果を診療録に記録する場合、図４の患者の健康医療情報データの編集欄１２２に書き込んで行く。大病院の場合は、既に電子カルテを導入している所もあるので、電子カルテに記載した内容をカット＆ペーストで貼り付けても良い。そして、編集欄１２２に書き込んだ内容は暗号化されてデータセンターへ送信される。

【００３９】データセンターでは、送信されてきた患者の健康医療情報データを解読して利用者の権限の範囲内か判断して利用者を特定可能な情報と共に保存する。利用者を特定可能な情報と共に保存したデータは所定の保存期間保存されるようになっており、削除および更新を端末装置側で行なってもそれは端末装置の画面上のみで、データセンターではどの部分を削除したという情報や、どの部分をどのような内容に置き換えたといった情報を追記していく形で、利用者を特定可能な情報と共に保存される。

【００４０】以上説明した実施例はあくまでも一例であり、利用形態に応じて種種の変形は可能であり、実施する時期の医療法に準じた範囲内で実施する必要がある。

【００４１】また、上述した実施例では、通信ネットワークとしてインターネットを前提としているが、専用回線を利用したクローズドネットワークを利用する方がセキュリティの面で有効であり、クローズドネットワークと暗号化を併用することも可能である。さらに、利用者権限によって、あるいは、通信される健康医療情報データに応じて通信ネットワークを使い分けることも可能である。

【００４２】また、端末装置側のプログラムをウェブブラウザの例で説明したが、ＨＴＭＬを利用した表現では表示可能な事項の制限が多く、さらに、入力に関しても制限が多くなってしまうので、専用のプログラムを作成するのが望ましい。また、上述の例では患者自身のログインと利用者のログインの双方を必要とするが、例えば、ＩＣカードに暗号化機能を有して患者自身のログインを省略することも可能である。さらに、利用者を登録する際に利用者アカウントを発行することで、ログイン画面において利用者アカウントでログインした場合には利用者の設定を省略することも可能である。さらに、利用者権限を個別に設定する例を示したが、医師，看護婦，薬剤師といった有資格者は、その資格を別途データベースとして登録してことも可能であり、利用者として登録するだけでそのデータベースから自動的に利用者権限が選択できるようにすることが可能であり、セキュリティの面においても操作性の面においても有効である。

【００４３】さらに、上述の実施例では個人が契約して、利用する例で説明したが、既に電子カルテを導入している病院で一括して登録してもよいし、市町村役場や健康管理組合などで一括して登録してもよい。さらに、データセンターは大病院のコンピュータを利用してもよいし、アウトソーシング事業を行なっているような委託された事業者でもよく、さらに、医療法が許す範囲で市町村役場や健康管理組合などで運用しても良い。

【００４４】（付記１）　個人の健康医療情報を電子データとして管理するデータ管理機能、利用者の権限および要求に応じ個人の健康医療情報データの一部ないし全てをネットワーク経由でアクセスできるアクセス機能を有し、健康医療情報データを共有できることを特徴とするヘルスケアデータ共有システム。

【００４５】（付記２）　個人健康医療情報の電子データを管理するデータ管理センターを設け、健康医療情報データを集中管理することを特徴とした、付記１のヘルスケアデータ共有システム。

【００４６】（付記３）　ヘルスケアデータ共有システムから取得した個人健康医療情報データを、追加、削除、更新を行うデータ追加機能、データ削除機能、データ更新機能の少なくとも１つを設け、個人健康情報データの追加、削除、更新の少なくとも１つが出来ることを特徴とする付記１、２のヘルスケアデータ共有システ

ム。

【００４７】（付記４）　ヘルスケアデータ共有システムから取得した個人健康医療情報データを、追加、削除、更新を行うデータ追加機能、データ削除機能、データ更新機能の少なくとも１つを端末装置側に設け、個人健康情報データの追加、削除、更新の少なくとも１つが出来ることを特徴とする付記１、２のヘルスケアデータ共有システム。

【００４８】（付記５）　健康医療情報データにアクセスしデータの取得、追加、削除、更新を行った場合、操作を行った利用者および日時などを特定できる操作記録機能を設け、データのアクセス内容、操作した利用者、操作日時の少なくとも１つの履歴が判ることを特徴とする付記１～４のヘルスケアデータ共有システム。

【００４９】（付記６）　付記５において、操作した利用者の情報にヘルスケアデータ共有システム利用者認証を使用する操作者認識機能を設け、操作した利用者の特定をすることを特徴とするヘルスケアデータ共有システム。

【００５０】（付記７）　利用者の権限を管理する利用者権限機能を設け、その権限に応じヘルスケアデータ共有システムから取得出来る情報、操作内容を制限すること特徴とする付記１～６のヘルスケアデータ共有システム。

【００５１】（付記８）　付記１～７の健康医療情報データに、診療データ、服薬データ、健康診断データおよび生体情報データの一部または全てを管理する各データ管理機能を設け、利用者の権限、要求によりデータの取得、追加、削除、更新できることを特徴とするヘルスケアデータ共有システム。

【００５２】（付記９）　健康医療情報データの他に個人に関わる情報（例えば家族歴、遺伝子情報等）の一部または全てを管理する個人情報管理機能を設け、利用者の権限、要求によりデータの取得、追加、削除、更新ができることを特徴とする付記１～８のヘルスケアデータ共有システム。

【００５３】（付記１０）　健康医療情報データの一部または全てを暗号化しデータを管理するデータ暗号化管理機能と、データをデータ管理機能より取得する際に暗号を解読するデータ解読管理機能を設け、データのセキュリティを高めることを特徴とする付記１～９のヘルスケアデータ共有システム。

【００５４】（付記１１）　健康医療情報データを通信ネットワーク経由で送受信する際に、送信するデータの一部または全てを暗号化するデータ暗号化機能と、受信した暗号データを解読するデータ解読機能を、端末装置とヘルスケアデータ共有システムの両方に設け、データのセキュリティを高めることを特徴とする付記１～９のヘルスケアデータ共有システム。

【００５５】（付記１２）　利用者が自分の健康医療情報データのセキュリティレベルを選択出来るセキュリティ選択機能を設け、健康医療情報データの一部ないし全ての暗号化有無を各自で設定出来ることを特徴とした付記１０、１１のヘルスケアデータ共有システム。

【００５６】（付記１３）　利用者の健康保険番号、クレジットカード等の情報を管理する健康保険管理、カード情報管理機能を設け、医療会計事務処理を行うこが出来ることを特徴とする付記１、２のヘルスケアデータ共有システム。

【００５７】（付記１４）　健康医療情報データの抽出、分析機能を設け、データの分析を行うことができることを特徴とする付記１、２のヘルスケアデータ共有システム。

【００５８】（付記１５）　個人の健康医療情報を電子データとして保存する健康医療情報データベースと、該健康医療情報データベースのアクセス制限を管理し、該健康医療情報データベースへの少なくとも記録を含む操作履歴を記録する操作履歴記録可能なセンター機能と、該健康医療情報データベースを利用する利用者を特定する認証機能と、通信ネットワーク経由で送受信するデータを暗号化および復号化するデータ暗号化機能とを有するヘルスケアデータ共有システムにおいて、前記通信ネットワークを経由してアクセスしてくる利用者を認証し、認証した利用者に対するアクセス制限の範囲で前記健康医療情報データベースの情報を暗号化して送信し、該送信した情報に対して追加、削除、更新された編集情報を受信して復号化して前記健康医療情報データベースに保存すると共に、前記認証機能で特定した利用者の操作履歴として記録することを特徴とするヘルスケアデータ共有方法。

【００５９】（付記１６）　個人の健康医療情報を電子データとして保存するヘルスケアデータ共有システムにアクセスするログインステップと、前記健康医療情報にアクセスする利用者を設定する利用者設定ステップと、前記ヘルスケアデータ共有システムから暗号化して送信されてきた健康医療情報データを復号化して表示する表示ステップと、前記表示された健康医療情報データを編集して、該編集した結果を暗号化して前記ヘルスケアデータ共有システムへ送信する送信ステップとからなることを特徴とするヘルスケアデータ共有プログラム

【００６０】

【発明の効果】以上説明したように本発明によれば、従来、医療機関などがそれぞれに非統一フォーマットで独自に管理していたため、集約的に管理することのできなかった個人の健康医療情報を、ネットワーク上のヘルスケアデータ共有システムで管理し、権限に応じた共有を行うことができ、実用的には極めて有効である。

【図面の簡単な説明】

【図１】通信ネットワークを介してアクセス可能なヘルスケアデータ共有システムの説明図。

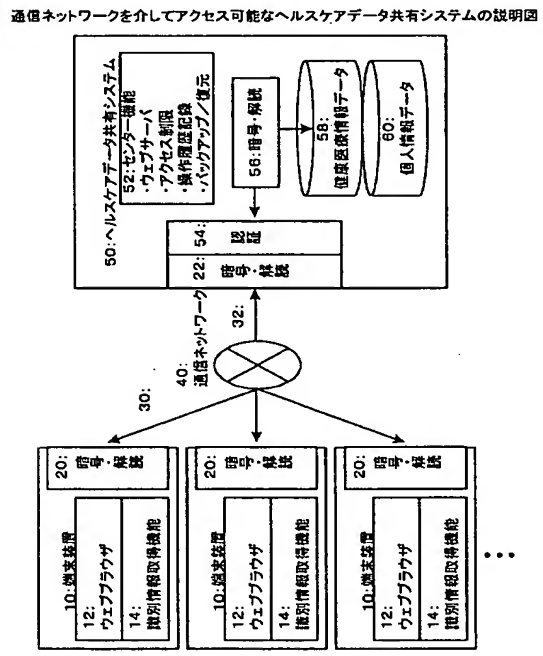
13

【図２】ヘルスケアデータ共有システムにアクセスする例を示す図。
【図３】ヘルスケアデータ共有システムの利用者を設定する例を示す図。
【図４】ヘルスケアデータ共有システムの表示例を示す図。
【図５】ヘルスケアデータ共有プログラムのフロー図。
【符号の説明】
１０　　端末装置
１２　　ウェブブラウザ

14

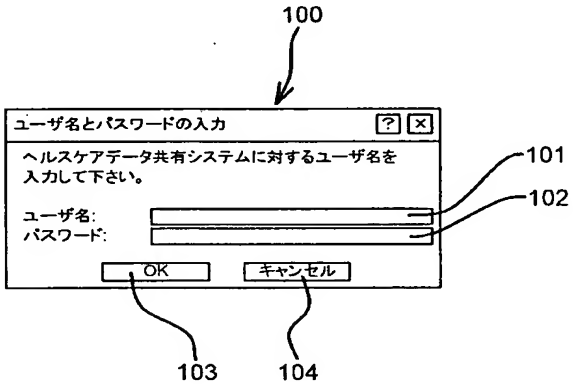
１４　　利用者識別情報取得機能
２０、２２通信経路のデータ暗号化／解読機能
３０、３２通信経路
４０　　通信ネットワーク
５０　　ヘルスケアデータ共有システム
５２　　センター機能
５４　　利用者認証機能
５６　　データ暗号化／解読機能
５８　　健康医療情報データ
６０　　個人情報データ

【図１】



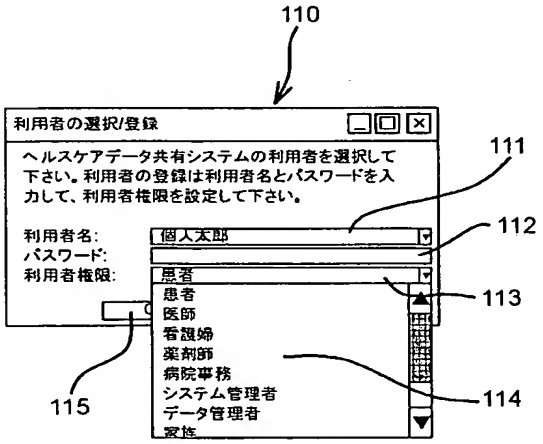
【図２】

ヘルスケアデータ共有システムにアクセスする例を示す図

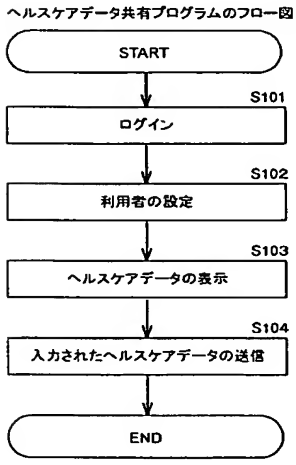


【図３】

ヘルスケアデータ共有システムの利用者を設定する例を示す図

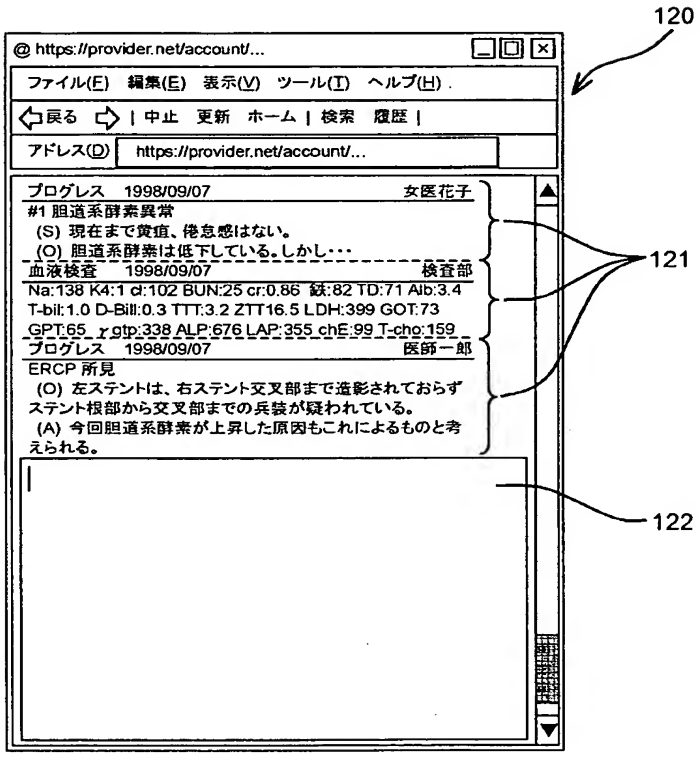


【図５】



【図４】

共有されたヘルスケアデータの表示例を示す図



フロントページの続き

(72)発明者　石井　雄一郎
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

(72)発明者　岩橋　秀祥
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

(72)発明者　阿曽沼　元博
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内